Chapter 7
Cyber-physical Systems Security

Md E. Karim and Vir V. Phoha

Introduction

Concerns with the security of the cyber-physical systems include the malicious attempts by an adversary to intercept, disrupt, defect or fail cyber-physical systems that may affect a large group of population, an important government agency or an influential business entity by denying availability of services, stealing sensitive data, or causing various types of damages, as well as the security breaches in small scale cyber-physical systems that may affect few individuals or relatively smaller entities [1, 2].

Large scale cyber-physical systems are vulnerable to physical attacks due to their wide exposures usually over a large geographic area. They are vulnerable to cyber attacks because of their network based accessibility that allows exploitation of systems vulnerabilities remotely. The integration of cyber and physical components in a cyber-physical system introduces another category of vulnerabilities that involves interception, replacement or removal of information from the communication channels. Thus, as shown in Fig. 7.1, the vulnerability space in a cyber-physical system includes a physical, a cyber and an integration component. In this paper we briefly describe the security issues, associated challenges and possible measures for each of these components.

M. E. Karim · V. V. Phoha (✉)
Center for Secure Cyberspace, Louisiana Tech University, Ruston, LA 71272, USA
e-mail: phoha@latech.edu

M. E. Karim
e-mail: mdekarim@latech.edu

S. C. Suh et al. (eds.), *Applied Cyber-Physical Systems*,
DOI: 10.1007/978-1-4614-7336-7_7,

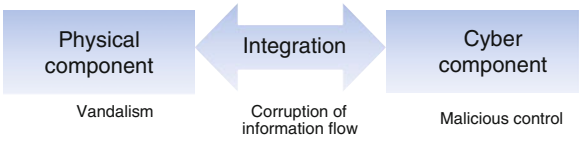

Fig. 7.1 Vulnerability space in a cyber-physical system

Physical Component

Large scale cyber-physical systems often involve physical infrastructures such as flow networks [3], and numerous data origination points. Sensors are spread over those points to capture the data generated. Collected data are then forwarded via networks to one or more central locations known as sinks or base stations. Those data are analyzed and appropriate responses are made, either locally at the sink or at a remote system.

Physical infrastructures such as pipelines are one of the weakest security links in a cyber-physical system. It is practically not possible, for most of the large scale cyber-physical systems, to protect their geographically dispersed physical infrastructures from vandalism. An adversary can damage an electric gridline, remove railway tracks or inject cyanide in a waterline. Each of these examples can have very serious consequences. Sensors designed to detect the indicators of possible violations of physical infrastructures can assist in identifying such vandalisms and minimize associated damages. This is particularly significant for large scale physical systems where immediate detection of vandalism is near impossible otherwise. However, the sensors, whether deployed to monitor vandalisms of physical infrastructure or to collect data from other critical data origination points, are themselves vulnerable to vandalism.

Sensor networks consist of many small components each of which is subject to physical capture. An adversary can remove or destroy the sensors from the field creating a coverage hole, as shown in Fig. 7.2, and disrupting transmission of critical data. It can also corrupt or replace sensors and inject erroneous data into the system and fail the decision making system that depends on those data.

Various schemes, primarily graph theoretical and anomaly detection based, have been proposed for detecting coverage holes or identifying compromised sensor nodes that can detect the absence, corruption or replay of sensor data leading to the detection of possible vandalisms. If sensor networks can withstand the attacks against the data encryption and replay prevention schemes then it should be difficult for an adversary to vandalize a sensor without an anomaly being noticed at the recipient end. Schemes for the detection of vandalisms in a sensor networks are not matured yet. It is expected that the effective automated monitoring of physical infrastructures as well as the sensor networks by identifying anomalies in the sensed input will be possible in the near future.

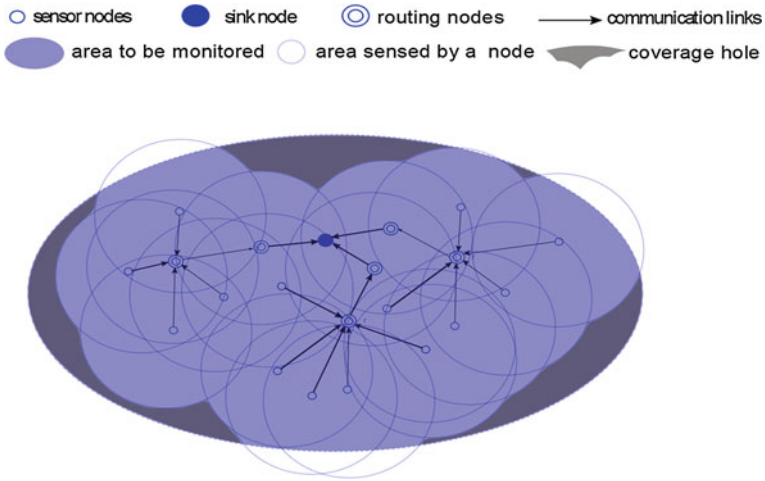

Fig. 7.2 The area *shaded gray* shows the coverage holes due to missing sensors

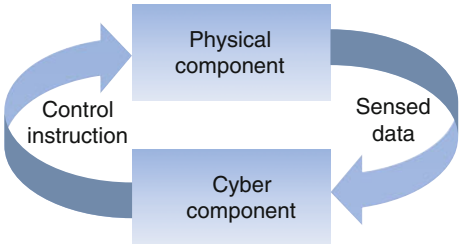

Fig. 7.3 The control loop in cyber-physical system

Cyber Component

Cyber component provides computational and control supports to cyber-physical systems (Fig. 7.3). It facilitates the fusion and analysis of data received from various sources and the overall decision making process. Remote network access that facilitates efficient interaction among various, possibly physically isolated, collaborating units of a cyber-physical system as well as efficient system administration, is an integral part of the cyber component. Such accessibility, however, also opens the door to the adversary for launching cyber attacks. These attacks may include: the denial of service, information corruption, destruction and exfiltration, and defective operation of the systems.

Denial of service attacks occur when an adversary creates an artificial mechanism, such as generation of frequent requests from a compromised distributed network, to keep the computing resources in the targeted system unnecessarily busy delaying or denying services to the legitimate requests [4]. Denial of service

attacks are common in cyber domain; a variation of them, referred to as denial of sleep attacks targets the battery life of the sensors by engaging with them frequently causing them to drain their batteries rapidly and die [5].

Various preventive and reactive measures have been proposed in the literature against denial of service attacks that are mostly based on the detection of deviation in the usage or traffic characteristics expected in a system. Protocol based solutions have been proposed against denial of sleep attacks for the sensor nodes by minimizing their responsiveness to random requests; a common approach is to designating a leader node in a cluster that interacts with the world external to that cluster and letting the rest of the nodes in that cluster periodically communicate with the leader. Different nodes in a cluster take turn as the leader so that a not does not die before the others.

Information corruption, destruction and exfiltration as well as defective operation of a system can be avoided if a system compromise can be detected and nullified. There have been numerous static, dynamic and hybrid (a combination of static and dynamic approaches) solutions that analyze patterns and signatures in program codes and behavior of the program executions and identify the presence of malicious agents in the systems and help the system administrator to disable them [6–9]. The static solutions are offline in nature and they include computing entropy or looking for specific signatures in codes, comparing programs with known malwares and analysis of disassembled codes for activity-space exploration. The dynamic solutions analyze the runtime behavior, such as system calls, of a program and block its execution if some suspicious sequence of operations is committed. While dynamic solutions work in real time, they cannot detect a malware if its behavior is not expressed. Many malware analysts prefer a hybrid solution to take advantage of the best of static and dynamic analyses. Malware authors obfuscate the code as well as the behavior of malware to defeat malware analysis. Deobfuscation of malware is one of the major primary concerns today that has been addressed through mathematical modeling, code transformation and normalization, and weighing on game-theoretical approaches by making obfuscation choices difficult for the adversaries instead of finding a full proof solution for them.

Different approaches have been proposed to detect intrusion in cyber systems, both at network level and host level. They operate either by an anomaly in network activity such as of bandwidth, ports and protocols, or comparing network flows with pre-determined attack signatures and may suffer from delays from the onset of the attacks to their detection. In real time cyber-physical systems, that have been increasingly using embedded systems, many intrusions can be detected through static timing analysis [10].

Unauthenticated access to a system by a disgruntled insider or an adversary having a stolen password is another dominant issue in cyber security. Behavioral biometric based solutions that analyze, say, a user's typing dynamics, mouse maneuvers or computer usage patterns have been proven to be effective against such attacks, although there have been some concerns whether these solutions can withstand sophisticated spoofing [11].

If outbound flow of information from a system that risks being compromised is forced to pass through a secure system, we can host a monitor in that secure system to detect and prevent information exfiltration. Some of the major approaches noticed in the literature to prevent information exfiltration include: (i) statistical testing based methods, (ii) keystroke/mouse-click association based methods, (iii) packet marking based methods, (iv) heuristic rule based filtering and (v) blacklist based egress filtering. The first four of these approaches largely remain vulnerable to mimic attacks and the blacklist based ones suffer from the requirement for frequent manual intervention and cannot guarantee sufficient completeness of the blacklist. Statistical testing based methods observe different statistical properties of malicious and benign traffic and train a classifier or an ensemble of classifiers for the future classification of unknown traffic [12]. Attributes most frequently used in statistical testing include: header signature, new connection establishment rate, packet size, upload/download bandwidth, ARP request rate, ICMP echo reply rate, request regularity, request time of the day and packet structure. Keystroke/mouse-click association based methods correlate the timing of keyboard or mouse activity to the timing of outbound traffic [13]. Packet marking based methods mark all outgoing requests at the application level [14]. A remote entity receiving and forwarding requests to the destination verifies if the requests are marked before they are forwarded. Firewalls operate based on heuristic rule sets with 50 average number of rules although about 1 % firewalls have 1000 or more rules [15]. A review on their limitations is available in [16]. NuFW, a new generation of firewall, uses senders' profiles to mitigate attacks such as insider threats and may help in preventing information exfiltration [17].

An adversary can defective operation of a cyber-physical system if it can compromise the control loop. Several solutions have been proposed on graceful degradation (where the system continue operating under failure) and survivability under such attacks [18].

Integration

Security issues involving integration space are very specific to cyber-physical systems and any discussion on the security of cyber-physical systems primarily focus on these issues. The main security issues in integration space involve security of flow of information [19–21]. There are numerous ways an adversary can intercept and exploit the communication from the physical sources to the sink (decision making unit) and vice versa.

An adversary can physically access or replace a node located at a critical point in a sensor network, or remotely update it with malicious code and take it over. It is difficult to locate and reset the compromised devices or reload the codes on them. In addition, responses to the failures in the subsystems with different ownership are difficult to coordinate.

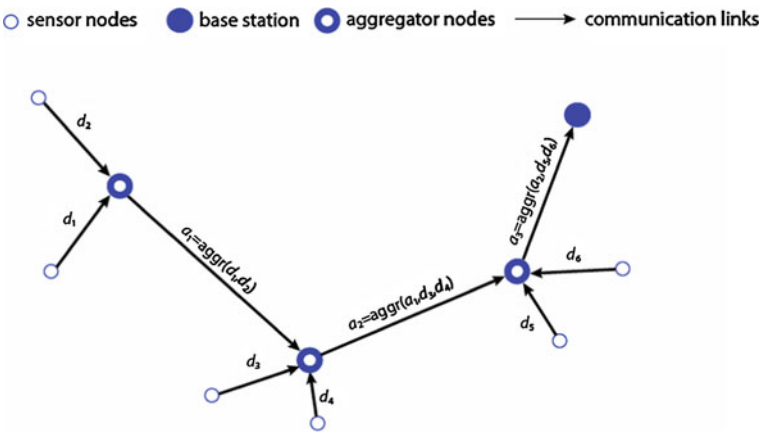

Fig. 7.4 Routing tree based data aggregation

Misleading information transmitted from the compromised nodes can lead to disastrous operation of cyber-physical systems. Many cyber-physical systems have real-time requirements and introduction of delay in the communication channel can result in cascading failures triggering one failure by the other [22–24]. Violation of confidentiality from the compromised nodes is another pressing issue that demands a satisfactory solution [25–27].

Since capture and compromise of a critical node in a sensor network is relatively easy, making a sensor network resilient under a compromise is the ideal solution that researchers are primarily seeking for.

Redundancy of the sensors is a common sense solution to many of the commonly encountered failures of sensors. However, in a sensor network, not all of the sensor nodes are equally important in terms of the value of information they contain and level of influence they have on the overall operation.

As shown in Fig. 7.4. Routing tree based data aggregation, in a typical sensor network based system data from different sources are aggregated at some intermediate nodes, known as data aggregators, on the way to the sink to filter out redundant data so that they get routed as fewer flows. This helps minimize the number of transmissions required to send the data to the sink, which in turn reduces the total energy spent by the network during the data transfers. In addition, it reduces the amount of bandwidth required for the data transfers.

As a consequence of the above schemes sensor located at a leaf node of the routing tree may have the least influence while a sensor located up above the routing tree and performing aggregation may be of high value. If an adversary can recognize high value sensors, it can selectively attack them without being overwhelmed by the abundance of the sensors. Being able to hide sensor network topology and routing infrastructure can make it difficult for an adversary to steal valuable information as well as corrupt massive amount of information [28]. For instance, the lesser association can be established between a terminal node and an

aggregator node, the better we can limit the opportunities for compromising the aggregator node (by making it difficult to recognize).

Schemes for hiding topology may make the job for an adversary difficult but they do not guaranty resilient operation of a sensor network. It is important that we are able to identify a node that is compromised [29, 30]. It is also important to adopt some encryption based trust management scheme that can identify with high confidence which of the sensor nodes may or may not be trusted. However, in a sensor network end-to-end encryption from the leaf nodes to the central base station is not possible because, as mentioned before, many nodes located in between aggregate data from the lower level of the topology that cannot be done with encrypted data. Lightweight key based encryption schemes that can assist trust management as well as support data aggregation is a challenge towards achieving resilience in sensor networks.

Conclusion

Security aspects and associated models for cyber-physical systems vary from systems to systems and researchers envision their unified future differently. The common objective is to make sure that the availability, integrity and the confidentiality of cyber-physical systems are maintained are under an attack by resisting the attack or recovering from it or, through graceful degradation [18]. Determining generic security policies for cyber-physical systems is an important first step towards achieving those objectives under different criteria [31]. Security-aware platforms [32] and protocols [33] as well as devices (such as secure cyber-physical couplings, resulted from the new advancements in semiconductor technologies [34]), designed with cyber-physical systems in mind are eventually going to determine how the security approaches to cyber-physical systems evolve in the future.

References

1. N. Adam, “Cyber-physical systems security,” presented at the Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee, 2009.
2. E. K. Wang, et al., “Security Issues and Challenges for Cyber-Physical System,” presented at the Proceedings of the 2010 IEEE/ACM Int’l Conference on Green Computing and Communications \& Int’l Conference on Cyber, Physical and Social Computing, 2010.
3. M. Yilin, et al., “Cyber-Physical Security of a Smart Grid Infrastructure,” *Proceedings of the IEEE,* vol. 100, pp. 195–209, 2012.
4. J. Mirkovic, et al., *Internet denial of service: attack and defense mechanisms*: Prentice Hall, 2005.

5. M. Brownfield, et al., "Wireless sensor network denial of sleep attack," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, 2005, pp. 356–364.
6. A. Dinaburg, et al., "Ether: malware analysis via hardware virtualization extensions," presented at the Proceedings of the 15th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2008.
7. M. I. Sharif, et al., "Impeding Malware Analysis Using Conditional Code Obfuscation," in *NDSS'08*, 2008.
8. C. Willems, et al., "Toward Automated Dynamic Malware Analysis Using CWSandbox," *Security & Privacy, IEEE,* vol. 5, pp. 32–39, 2007.
9. A. Moser, et al., "Exploring Multiple Execution Paths for Malware Analysis," in *Security and Privacy, 2007. SP '07. IEEE Symposium on*, 2007, pp. 231–245.
10. C. Zimmer, et al., "Time-based intrusion detection in cyber-physical systems," presented at the Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, Stockholm, Sweden, 2010.
11. R. Chow, et al., "Enhancing cyber-physical security through data patterns," in *Proceedings of the Workshop on Foundations of Dependable and Secure Cyber-Physical Systems*, 2011.
12. B. Thuraisingham, "Data mining for security applications: Mining concept-drifting data streams to detect peer to peer botnet traffic," in *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*, 2008, pp. xxix–xxx.
13. R. Gummadi, et al., "Not-a-Bot: improving service availability in the face of botnet attacks," presented at the Proceedings of the 6th USENIX symposium on Networked systems design and implementation, Boston, Massachusetts, 2009.
14. K. Xu, et al., "Data-Provenance Verification For Secure Hosts," *IEEE Trans. Dependable Secur. Comput.,* vol. 9, pp. 173–183, 2012.
15. P. Gupta, "Algorithms for routing lookups and packet classification," PhD Thesis, Stanford University, Stanford, CA, USA, 2000.
16. A. X. Liu and M. G. Gouda, "Diverse Firewall Design," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 19, pp. 1237–1251, 2008.
17. N. C. Team, "NuFW firewall: Now User Filtering Works," 2008.
18. A. A. Cardenas, et al., "Secure Control: Towards Survivable Cyber-Physical Systems," in *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*, 2008, pp. 495–500.
19. R. Akella, et al., "Analysis of information flow security in cyber–physical systems," *International Journal of Critical Infrastructure Protection,* vol. 3, pp. 157–173, 2010.
20. T. T. Gamage, et al., "Enforcing Information Flow Security Properties in Cyber-Physical Systems: A Generalized Framework Based on Compensation," presented at the Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, 2010.
21. T. Gamage, et al., "Information flow security in cyber-physical systems," presented at the Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tennessee, 2011.
22. C. Neuman, "Challenges in Security for Cyber-Physical Systems," in *Workshop on Future Directions in Cyber-physical Systems Security*, 2009.
23. H. Tang and B. M. McMillin, "Security Property Violation in CPS through Timing," presented at the Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems Workshops, 2008.
24. F. Mueller, "Challenges for Cyber-Physical Systems: Security, Timing Analysis and Soft Error Protection," in *Proc. of the National Workshop on High Confidence Software Platforms for Cyber-Physical Systems*, 2008.
25. T. T. Gamage, et al., "Confidentiality Preserving Security Properties for Cyber-Physical Systems," presented at the Proceedings of the 2011 IEEE 35th Annual Computer Software and Applications Conference, 2011.

26. T. Kohno, "Security for cyber-physical systems: case studies with medical devices, robots, and automobiles," presented at the Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, Tucson, Arizona, USA, 2012.
27. R. Mitchell and I.-R. Chen, "Behavior Rule Based Intrusion Detection for Supporting Secure Medical Cyber Physical Systems," in *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, 2012, pp. 1–7.
28. Z. Quanyan, et al., "A hierarchical security architecture for cyber-physical systems," in *Resilient Control Systems (ISRCS), 2011 4th International Symposium on*, 2011, pp. 15–20.
29. M. Mathews, et al., "Detecting Compromised Nodes in Wireless Sensor Networks," in *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on*, 2007, pp. 273–278.
30. P. R. Nalabolu, "Detecting Malicious Code in Sensor Network Applications Using Petri Nets," M.S., Oklahoma State University, Oklahoma City, OK, USA, 2007.
31. K. K. Fletcher and L. Xiaoqing, "Security Requirements Analysis, Specification, Prioritization and Policy Development in Cyber-Physical Systems," in *Secure Software Integration & Reliability Improvement Companion (SSIRI-C), 2011 5th International Conference on*, 2011, pp. 106–113.
32. M. Azab and M. Eltoweissy, "Defense as a service cloud for Cyber-Physical Systems," in *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*, 2011, pp. 392–401.
33. G. S. Lee and B. Thuraisingham, "Cyber-physical systems security applied to telesurgical robotics," *Comput. Stand. Interfaces,* vol. 34, pp. 225–229, 2012.
34. O. Al Ibrahim and S. Nair, "Cyber-physical security using system-level PUFs," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, 2011, pp. 1672–1676.